International Journal of Management (IJM)
Volume 11, Issue 8, August 2020, pp. 2204-2215, Article ID: IJM_11_08_191
Available online at http://www.iaeme.com/IJM/issues.asp?JType=IJM&VType=11&IType=8
Journal Impact Factor (2020): 10.1471 (Calculated by GISI) www.jifactor.com
ISSN Print: 0976-6502 and ISSN Online: 0976-6510
DOI: https://doi.org/10.34218/IJM.11.8.2020.191

RECOGNITION AND AVOIDANCE OF BLACKHOLE AND GRAYHOLE ATTACKS IN MANET

Anu Sharma[1], Dr. Jitendra Sheetlani [2]

[1]Research Scholar, Department of Computer Science,
Sri Satya Sai University of Technology and Medical Sciences at Sehore, Madhya Pradesh, India

[2]Associate Professor, Department of Computer Science,
Sri Satya Sai University of Technology and Medical Sciences at Sehore, Madhya Pradesh, India

ABSTRACT

Security of the data transmission process on the Mobile Ad Hoc network (MANET) is very important, but wireless communication, dynamic topology changes Limited resources and the absence of centralized settings make MANET vulnerable to all kinds of DoS attacks at the network layer such as Grayhole and Blackhole which can disrupt the data transmission process by discarding received packets. This paper describes the security mechanism to detect and fight Grayhole and Blackhole attacks on one of the routing protocols in MANET, namely AODV

Key words: Security, Blackhole Attack, Grayhole Attack, AODV, MANET

Cite this Article: Anu Sharma and Jitendra Sheetlani, Recognition and Avoidance of Blackhole and Grayhole Attacks in Manet, *International Journal of Management (IJM)*, 11(8), 2020, pp. 2204-2215.
http://www.iaeme.com/IJM/issues.asp?JType=IJM&VType=11&IType=8

1. INTRODUCTION

Mobile Ad Hoc Network is a network consisting of several nodes that coordinate and converse with each other. Each node has a limited range so that the concept of multi-hop forwarding is used where each node operates like a router that can forward packets to other nodes on the network. MANET is widely applied to military communications, automated war equipment, disaster relief teams, police, firefighters, and as a communication tool when communication infrastructure is damaged by natural disasters. The nodes in MANET communicate wirelessly and have movement at a certain speed which causes an ever-changing network topology. MANET has other characteristics such as limited bandwidth, battery capacity, and low computing power [1, 2].

Although the characteristics possessed by MANET are needed for network flexibility, they are also a problem factor in MANET such as IP addressing problems, radio interference, routing protocols, power limitations, the need for movement management, QoS, and network security. Where security issues in MANET are things that must be considered because MANET is sufficiently susceptible to different types of attacks such as eavesdrop, interference, masquerade, and denial of service [3]. Where one or more nodes on the network can carry out attacks without being detected first. Attacking nodes can send incorrect routing packets, provide incorrect route information or even flood other nodes which will increase network traffic. [4] The two types of DoS attacks on MANET are Grayhole and Blackhole. In a black hole attack, the attacker node will discard all received packets, while a gray hole is a variation of black holes where the node will attack by discarding received packets at a certain time interval and will behave normally like other nodes.

To deal with security problems due to Blackhole and Grayhole attacks on the AODV routing protocol in MANET, a method is designed to detect and remove both types of attacks from the network [5]. The mechanism used consists of several security procedures, namely Neighbourhood information compilation; Local abnormality discovery; Cooperative abnormality discovery; Global Alarm Raiser. In this mechanism, there are several changes to the routing protocol used, namely each node stores a routing table along with a list of attacker nodes. Information about the attacker's node is sent with the RREP and RREQ packets,

2. LITERATURE STUDY

2.1 Ad Hoc On-Demand Distance Vector (AODV)

Adhoc On-Demand Distance Vector (AODV) is a reactive protocol on MANET that operates on demand. Routes between nodes on the network s formed whilst the resource node needs to throw a packet to the destination node. The node will store a routing table with a list of one destination node with only one route [11]. Routes that are not used at certain intervals will be removed from the table. The routing process in AODV is divided into two, route discovery using Route Request (RREQ) and route reply (RREP) packets, and route maintenance using route error (RERR) packets. The following are the RREQ and RREP package formats.

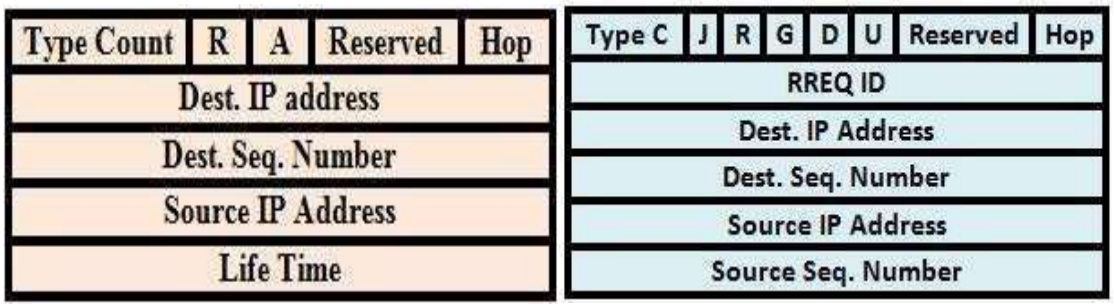

Figure 1 RREQ and RREP Package Formats

The route discovery process consists of two methods, source routing, and backward learning. In source routing, the source node will broadcast the RREQ packet to all nodes neighbours with the address of the destination node. The neighbouring node will re-broadcast RREQ packets to its neighbouring nodes. Each node on the network will check the routing table to find out whether it is the destination node or has a route to reach the destination node. If the node is not the destination node, the RREQ packet will be forwarded. At the same time as the RREQ broadcast, a reverse path is formed.

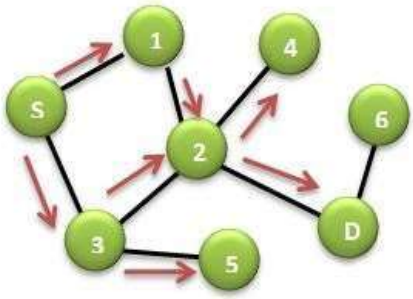

Figure 2 RREQ Package Delivery Process

Intermediate nodes that have routes to destination nodes or the destination node that receives the RREQ can reply by sending RREP packets to the source node unicast using the reverse path that has been formed or also called backward learning. Reverse path used by the destination node to reach the source node which will be the route to reach the destination node [3].

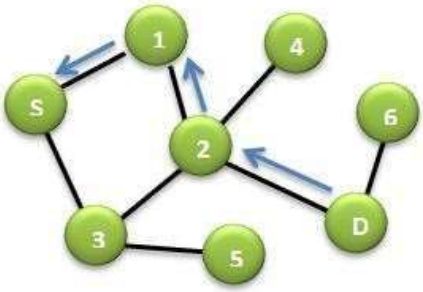

Figure 3 RREP Package Delivery Process

After the route to the destination, the node is established, the source node responsible for maintaining existing routes. If there is damage or failure, the RERR packet will be broadcast by the node that has failed to all nodes on the network until it reaches the source node.

2.2 Network Security

Several mechanisms can be used to provide solutions to network security by preventing, detecting, or responding to attacks on the network. The mechanism provided must prioritize availability where the network is only available to authenticated users; confidentiality where the confidentiality of information must be maintained; integrity where the transmission process must be protected from all kinds of attacks; authentication where the network can only be accessed by authenticated nodes [6]. Several categories of attacks on the network are such as Passive Attack; Active Attack; External Attack; Internal Attack

AODV is vulnerable to attacks where attackers can discard packets, modify packet formats and forward them, send fake packets after receiving routing packets or send fake packets without receiving routing packets first. Attacking nodes can fake RREP packets by setting the hop count value to 1; amplify the destination series number to at least 1; sets the resource IP address to a non-existent IP address, sending a spoofed RREP packet to the source node to obtain a route from the source node [4].

2.3 Black Hole Attack

Blackhole attacks can be divided into two categories, group attacks carried out by more than one attacker node working together and individual attacks carried out by only one attacker node

[7]. In a black hole assault, the assailant node obtains the desired route by stating to the source node that it has the shortest route to reach the destination node. After receiving an RREQ packet, the attacker node immediately sends a fake RREP packet to the source node without seeing any information about the destination node. The attacker node manipulates the RREP by providing a false sequence number and hops count stating that the attacker node has the shortest and most recent route.

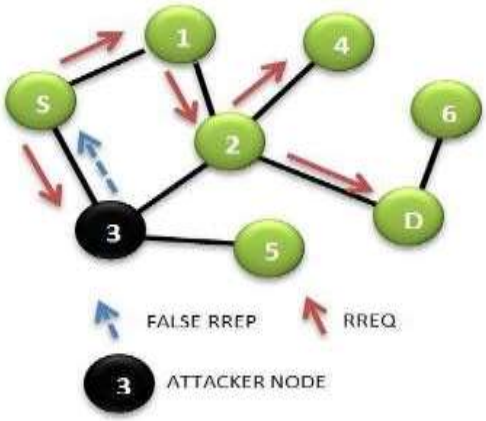

Figure 4 Attacker Node Sends False RREP

With a high destination node sequence number value and RREP packet that is first received by the source node. The source node will reject RREP packets sent by other nodes even though it has the correct route. So the route between the source node and the attacker node will be formed and the source node will start sending packets to the attacker node. The attacker node then starts dumping the received packets [3].

2.4 Gray Hole Attack

A gray hole attack is a variation of a blackhole attack where the attacker node will discard received packets selectively and with a certain pattern. [6] Nodes the attacker can perform an attack by discarding all UDP packets and forwarding TCP packets or vice versa or the attacker node can discard all packets with a certain probability.

Attacking nodes can also carry out attacks by discarding all incoming packets destined for the node on the network but will forward all incoming packets destined for other nodes. In addition, the attacker node can also discard all packets at a certain time and will return to behaving like normal nodes. With the characteristics of these attacks, the attacker node that launches the gray hole attack will be difficult to detect.

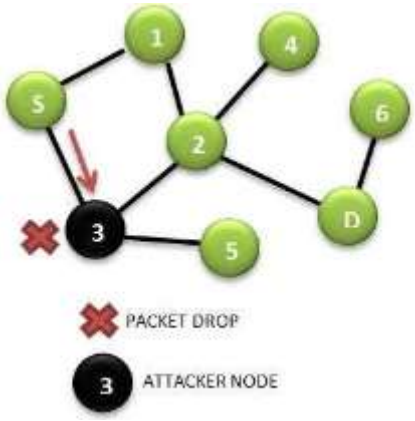

Figure 5 Attacker Node Dispose Received Packages

3. PREVIOUS RESEARCHES

Secure AODV protocol [8] is used to reduce the impact of black hole attacks by utilizing feedback from neighboring nodes before forwarding data packets to other nodes. The decision is taken based on the number of RREQ and RREP packets that are successfully forwarded by a node so that it can be known whether the node is a malicious node or an ordinary node.

Oscar et al [9] also use the concept of limit value to find dangerous nodes by observing the behavior of nodes. If the node does not comply with the rules continuously until it exceeds the limit value, it will be declared a dangerous node. In this method, it takes time to get all the data that is needed to be required to identify and declare a node as a malicious node. In addition, malicious nodes can still discard packets before being declared a malicious node.

The concept of using a limit value is carried out in the DPRAODV protocol [10] by using an ALARM packet that contains a list of malicious nodes that will be sent to neighboring nodes to inform that RREP packets from malicious nodes to be discarded. By using this protocol there will be an increase in overhead due to the addition of the ALARM package. Using this method will take longer.

Piyush et al. [11] provides a solution where the source and destination nodes perform end-to-end checks to determine whether the data packet has been received by the destination node or not. If the checking process fails, a checking process for malicious nodes will be carried out. The proposed solution can only operate with the assumption that each node on the network has a level of trust in each other as normal nodes rather than considering it as an attacker node. In addition, if the number of attacker nodes is more than expected, the accepted solution becomes vulnerable to attacks.

Ochola et al. [12] offers a mechanism to detect the presence of malicious nodes. When the source node receives the RREP packet, it will verify the intermediate nodes on the route to the destination node whether the node is the right one sending the RREP packet does have a route to reach the destination node and other intermediate nodes. Otherwise, the node will be declared as a malicious node. By using this algorithm, a black hole attack can be detected if it is only carried out by one attacker node. If the attack is carried out by more than one attacker node, it will be vulnerable to attack. In addition, there is also an end-to-end delay due to the verification process carried out by the source node.

4. PROPOSED DESIGN

The MANET network used consists of nodes of the same type that can move freely or stay at a certain location at certain intervals of time. Any node can join and leave the network and run into problems at any time. The nodes on the network communicate peer-to-peer wirelessly with multi-hop and bandwidth limitations. Each node has a Nonzero ID where all links on the network are bi-directional. On the network, it is possible to have more than one attacker node that will carry out the gray hole and black hole attacks.

The detection mechanism offered consists of local and global detection and network notification of the presence of attacker nodes that have been detected. Thus the attacker node can be isolated and not permitted to use network assets. The detection method comprises of four processes that work sequentially, namely: 1) Neighbor Node Data Collection; 2) Local Detection; 3) Global Detection; 4) Global Alert

4.1 Neighbor Node Data Collection

In the process of collecting neighboring nodes, the nodes on the network which are referred to as the Initiator Node (IN) will collect routing information carried out by each neighbor node. The information that has been obtained will be stored in a routing information table

consisting of five columns, namely NodeID, FROM, TO, RTS/CTS, CHECK BIT. The NodeID column shows the neighboring nodes. In column FROM marked '1' if it has forwarded packets coming from that node. While the KE column is marked '1' if it has forwarded the packet to that node. RTS/CTS (Request to Send/Clear to Send) is the ratio between the number of requests received by a node and the number of packets transmitted by that node. The Check bit column will be marked '1' if the ProbeCheck packet has been received by the Initiator Node from a certain neighboring node.

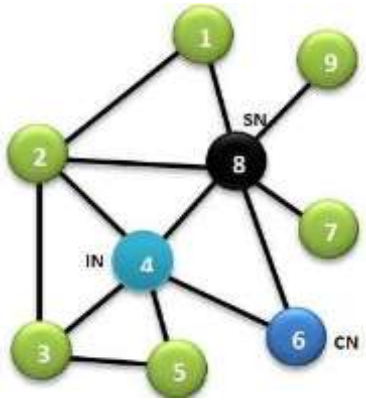

Figure 6 Network used

By using a network topology as shown in Figure 7 with node 4 as IN, the Routing Information Table for node 4 is as follows:

Table 1 Routing Information Table

NodeID	From	KE	RTS/CTS	CHECKBIT
2	0	1	2	1
3	0	0	5	0
5	1	0	6	1
6	1	1	4	0
8	0	0	10	1

After IN creates a routing information table, IN will analyze it to find neighboring nodes that have not communicated with it at a certain time interval. IN will look for neighboring nodes that have a value of '0' in the FROM and TO columns and with a high RTS/CTS value. After IN determines the suspected attacker node or Suspected Node (SN), IN will run the next process, namely Local Detection.

4.2 Local Detect

In local detection, IN will select Cooperative Node (CN) from neighboring nodes by referring to the Routing Information Table. IN will select the node that has the value '1' in the FROM and TO columns to be CN. After specifying the CN, IN will broadcast the RREQ packet to neighboring nodes 1 hop away requesting a route to the CN. IN will receive RREP packets from neighboring nodes and also from the Suspected Node (SN) that is suspected of carrying out an attack. IN will send ProbeCheck packet to CN via SN with certain Time to Live (TTL) value after receiving RREP packet from SN. After the TTL value of the package is exhausted, IN will ask the CN whether the CN has received the ProbeCheck package or not. If the CN has received the ProbeCheck packet, In will give the value '1' in the CheckBit column for the CN node in the Routing Information Table which means SN not proven to be an attacker node at that time.

Meanwhile, if the CN does not receive the ProbeCheck packet, the IN will raise suspicion on the SN and run the next process, namely Global Detection.

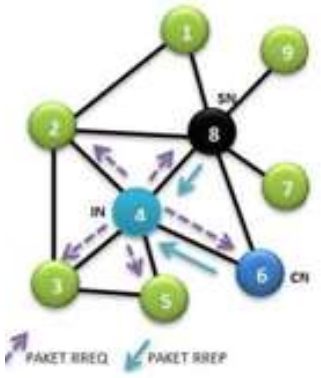

Figure 7 Route request to CN by IN

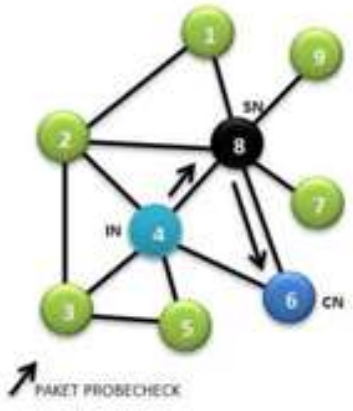

Figure 8 Package Delivery Probe Check

4.3 Global Detection

The Global Detection Process is carried out to increase the reliability of the local detection process reduce the probability of error in detection due to link failure. In this process, IN will send Cooperative Detection Request (CDREQ) packets to all nodes neighbors. SN neighbor node will send RREQ packet to SN after receiving CDREQ packet to request a route to IN. The neighboring node of the SN will send a FurtherProbe (FRPROBE) packet to IN via the route given by Sn to the RREP packet in response to the RREQ packet. In addition to sending FRPORBE packets, neighboring nodes also sends NOTIFY packets to IN which means that FRPORBE packets have been sent to IN. Sending NOTIFY packets to use a route that does not go through SN.

After receiving the FRPROBE and NOTIFY packets, IN will create a ProbeCheck table containing the NodeID and ProbeStatus. Where nodeID indicates which node sent a NOTIFY packet and ProbeStatus is '1' if the IN node has received a FRPROBE packet from that node. Each node will send three FRPROBE packets at narrow intervals. This case does for reduce the probability that the FRPROBE packet does not reach INdue to collision, buffer overflow, or another link failure. If the IN does not receive the three FRPROBE packets, then the SN is declared as the attacker node in that time frame and the SN will be isolated from the network through the next process, namely Global Alert.

4.4 Global Alert

The Global Alert process is used to provide network-wide alerts of the presence of detected attacker nodes. After the attacker node is detected, the node on the network will send a GLOBALARM packet which is signed as a private key to all neighboring nodes. After all k nodes on the network have signed their respective private keys in the GLOBALARM package, the attacker node will be isolated from the network. The nodeID of the attacker's node will be entered in the Attacker List which contains the attacker's nodes that have been detected. The list will be updated periodically if there are changes. Where the propagation process of the Attacker List can be done in two ways, the first by broadcasting to all nodes by riding on the RREQ and RREP packets. Second, each node only stores a partial Attacker List, which only contains neighboring nodes1 hop and only updated if there is a change in the neighboring node.

5. RESULTS AND ANALYSIS

5.1 Effect of Design Parameters on Throughput

The design parameters to be tested have an effect on the *throughput* are network size, packet injection rate, packet size, buffer size. With design parameters that vary in value, comparisons are made for the different flow control methods used.

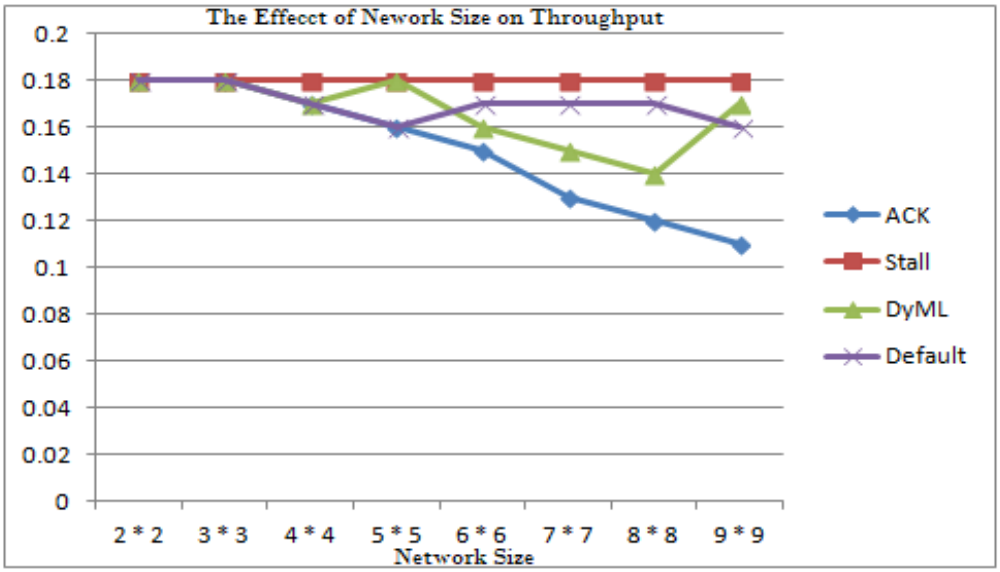

Figure 9 Graph of the Effect of Network Size on Throughput

Table 2 Probe Check. Table

NodeID	Probe Status
2	1
3	1
5	1
6	0

That increasing the network size from 2 x 2 to 8 x 8 causes changes in the throughput value. For networks with default flow control, the larger the network size causes throughput

to decrease, throughput changes begin to decrease significantly when the network size is 5 x 5 with the current throughput value of 0.15779 flits/cycle and throughput decreasing by 0.0187 flits/cycle with a decreasing rate up to 8 x 8 network size is equal to 0.013387 flits/cycle/network size. This is because throughput is calculated in units of flits/cycle, with packet size, buffer size, and packet injection rate being fixed. If the network size is enlarged, the time required for a flit to reach its destination will increase, causing throughput to decrease. In addition, the only shipping method allowing sending 1 flit before receiving an ack is one of the factors that reduce throughput when the network size is enlarged.

5.2 Effect of Design Parameters on Delay

One of the network performance parameters observed is a delay which is calculated in cycles. delays related to several design parameters, which were tested using 3 flow control methods to obtain their effect on changes in delay. It is expected that a network has a low delay. Figure 10 and Figure 11 show the results of the effect the size of the network those changes with the delay that occurs on the network

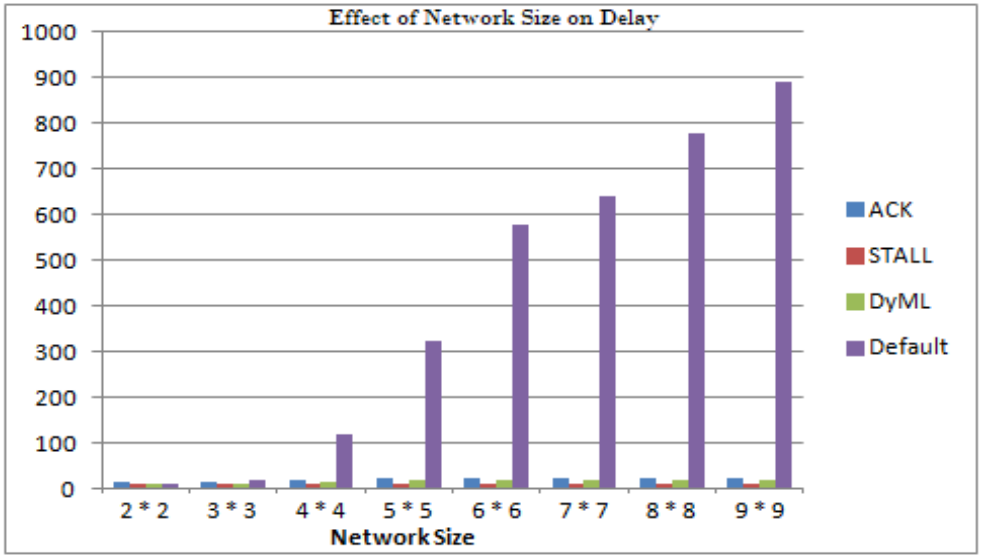

Figure 10 Effect of Network Size on Delay

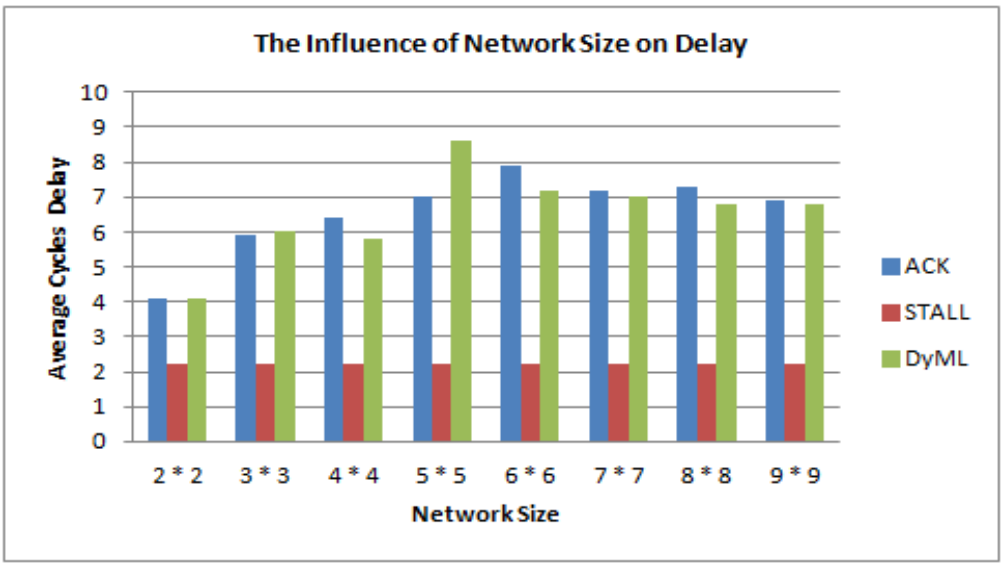

Figure 11 Influence Traffic Network Size against Delay

That the influence of network size on delay and comparison of three flow control methods are obtained where different results are obtained for each flow control used. Delay is directly proportional to the size of the network on a network that uses the default flow control. While the network uses Stall flow control, changes in network size do not have a significant effect. While the flow control Ack and DyML experience an increase in the delay until the network size is 5x5 and then the delay decreases when the network size is increased.

For networks that use the default flow control, the increase in delay that occurs is 126.79 cycles with the delay that occurs on a network size of 9x9 is 893.02 cycles. When the network size is 5x5, the biggest delay increase is 210.44 cycles.

For flow control stalls, with increasing network size, tend not to have a significant impact on network delay. The average delay that occurs is 2,239 cycles with the delay that occurs when the network size is 9 x 9 in 2,243 cycles. Meanwhile, DyML and Ack flow control have almost the same characteristics, where there is an increase in delay along with the increase in network size, and at the same time, a certain network size is achieved the maximum delay before the delay that occurs in the network decreases as the network size increases.

5.3 Effect of Design Parameters on Power Used

In the network many components and factors that can affect power usages such as routing algorithms, selection functions used, and router conditions. So that by increasing the size of the network, it will have an impact on increasing the use of power on the network, both those that apply default flow control and those that apply other flow control methods.

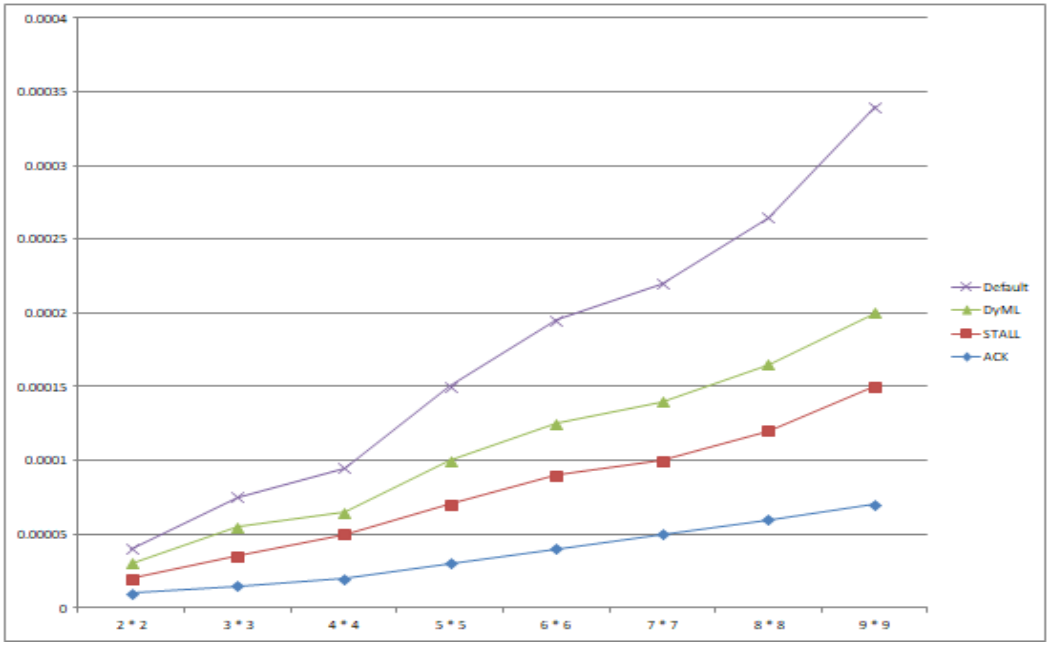

Figure 12 Graph of Size Effect Network against Power

6. CONCLUSION

The conclusions that can be drawn from this study after measuring and analysing the data from the results of the three flow control methods obtained are:

- Flow Control Stall / Go, Ack / Nack, and DyML affect the network that is experiencing saturation

- With the combination of Packet Injection Rate design parameters and buffer size, Stall / Go, Ack / Nack and DyML flow control does not cause saturation until the packet injection rate used is 0.3
- With a combination of design parameters Package Size and Packet Injection Rate, Stall / Go, Ack / Nack and DyML flow control does not cause saturation until the packet size used is 20 – 22 flit.
- With a combination of design parameters Packet Size and Packet Injection Rate flow control, Ack/Nack and DyML achieve the largest throughput when packet sizes are 8 – 10 flit.
- To increase throughput, the Packet Injection Rate, Packet Size, Buffer Size, and Network Size must be enlarged,
- To reduce the delay, the Packet Injection Rate, Packet Size, and Network Size must be reduced by increasing the Buffer Size
- To reduce power consumption, the Packet Injection Rate, Packet Size, Buffer Size, and Network Size must be reduced.

REFERENCES

[1] Idrees, Muhammad. (2021). Mobile Ad Hoc Network.

[2] Loo, Jonathan & Khan, Shafiullah & Al-Khwildi, Ali. (2016). Mobile Ad Hoc Network. 10.1201/b11447-2.

[3] Lohi, C., & Sharma, S. (2014). A Survey of Mitigation Techniques to Black Hole Attack and Gray Hole Attack in MANET. https://api.semanticscholar.org/CorpusID:14333284

[4] Vivek, Usha & Sundan, Bose. (2012). Comparing the impact of black hole and gray hole attacks in mobile adhoc networks. Journal of Computer Science. 8. 1788-1802. 10.3844/jcssp.2012.1788.1802.

[5] Kaur, Rupinder & Singh, Parminder. (2014). Review of Black Hole and Grey Hole Attack. The International journal of Multimedia & Its Applications. 6. 35-45. 10.5121/ijma.2014.6603.

[6] V.Shanmuganathan, Mr.T.Anand M.E, A Survey on Gray Hole Attack in MANET,IRACST International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501 Vol.2, No6, December 2012

[7] Tseng, Fan-Hsun & Chou, Li-Der. (2011). A survey of black hole attacks in wireless mobile Ad hoc networks. Human-centric Computing and Information Sciences. 1. 10.1186/2192-1962-1-4.

[8] K. S. Sujatha, V. Dharmar and R. S. Bhuvaneswaran, "Design of genetic algorithm based IDS for MANET," 2012 International Conference on Recent Trends in Information Technology, 2012, pp. 28-33, doi: 10.1109/ICRTIT.2012.6206796.

[9] Gonzalez, Oscar & Ansa, Godwin & Howarth, Michael & Pavlou, George. (2008). Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks. J of Internet Engineering. 2. 181-192. 10.1007/978-3-540-72697-5_26.

[10] Raj, Payal & Swadas, Prashant. (2009). DPRAODV: a dynamic learning system against blackhole attack in AODV based MANET. International Journal of Computer Science Issues. 2.

[11] Piyush Agrawal, R. K. Ghosh, and Sajal K. Das. 2008. Cooperative black and gray hole attacks in mobile ad hoc networks. In Proceedings of the 2nd international conference on Ubiquitous information management and communication (ICUIMC '08). Association for Computing Machinery, New York, NY, USA, 310–314. DOI:https://doi.org/10.1145/1352793.1352859

[12] Ochola, Elisha & Mejaele, L.F. & Eloff, Mm & Van der Poll, John. (2017). Manet Reactive Routing Protocols Node Mobility Variation Effect in Analysing the Impact of Black Hole Attack. SAIEE Africa Research Journal. 108. 80-91. 10.23919/SAIEE.2017.8531629.